网络卫士防火墙系统
安装手册

天融信

TOPSEC®

北京市海淀区上地东路 1 号华控大厦，100085

电话：(86)10-82776666

传真：(86)10-82776677

服务热线：800-810-5119

http: //www.topsec.com.cn

版权声明

本手册中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有　不得翻印©　2007 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信公司

信息反馈

http://www.topsec.com.cn

目　录

1　前言 1

1.1　文档目的 1
1.2　读者对象 1
1.3　文档组织 1
1.4　约定 1
1.5　相关文档 2
1.6　技术支持 2

2　安装网络卫士防火墙 4

2.1　系统组成与规格 4
2.1.1　系统组成 4
2.1.2　系统规格 4
2.2　确定防火墙的工作模式 4
2.3　系统安装 5
2.3.1　硬件设备安装 5
2.3.2　管理器安装 6
2.3.3　检查网络卫士防火墙的工作状态 11
2.4　登录网络卫士防火墙 11
2.4.1　缺省出厂配置 11
2.4.2　使用CONSOLE口登录网络卫士防火墙 12
2.4.3　设置其他管理方式 15
2.4.4　管理主机的相关设置 18
2.4.5　通过浏览器登录防火墙 19
2.4.6　使用集中管理器登录防火墙 19
2.4.7　通过SSH方式登录网络卫士防火墙 21
2.5　恢复出厂配置 22

3　配置案例 23

3.1　案例 1：路由模式下通过专线访问外网 24
3.2　案例 2：混合模式下通过ADSL拨号访问外网 26
3.3　案例 3：建立VPN隧道 29

附录 A　扩展模块 32

1 前言

本安装手册主要介绍网络卫士防火墙的安装和使用。通过阅读本文档，用户可以了解如何正确地在网络中安装网络卫士防火墙，并进行简单配置。

本章内容主要包括：

- 本文档的用途
  - 阅读对象
  - 本文档的组织结构
  - 本文档的基本约定
  - 相关文档
  - 如何联系天融信技术支持

1.1 文档目的

本文档主要介绍如何安装网络卫士防火墙及其相关组件，包括设备安装、集中管理器安装和扩展模块安装等。

1.2 读者对象

本安装手册适用于具有基本网络知识的系统管理员和网络管理员阅读，通过阅读本文档，他们可以独自完成以下一些工作：

- 初次使用和安装网络卫士防火墙。
- 管理网络卫士防火墙。

1.3 文档组织

本文档包括以下章节及其主要内容：

- 网络卫士防火墙安装指南。介绍网络卫士防火墙系统的安装（硬件和管理系统），提供三个基本的配置范例，说明如何将网络卫士防火墙集成到网络中。
- 扩展模块的相关介绍（包括：百兆接口扩展模块、标准千兆模块和专用千兆模块）。

1.4 约定

本文档遵循以下约定：

命令语法描述采用以下约定，

尖括号（<>）表示该命令参数为必选项。

方括号（[]）表示该命令参数是可选项。

竖线（|）隔开多个相互独立的备选参数。

黑体表示需要用户输入的命令或关键字，例如 **help** 命令。

*斜体*表示需要用户提供实际值的参数。

图形界面操作的描述采用以下约定：

黑体表示“**按钮**”或菜单项。

点击（选择）一个菜单项采用如下约定：

点击（选择） **高级管理** > **特殊对象** > **用户**。

为了叙述方便，本文档采用了大量网络拓扑图，图中的图标用于指明天融信和通用的网络设备、外设和其他设备，以下图标注释说明了这些图标代表什么设备：

文档中出现的提示、警告、说明等，是关于用户在安装和配置网络卫士防火墙过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置操作。

提示 说明 实例 警告

1.5 相关文档

《网络卫士防火墙系统用户手册》

《网络卫士防火墙系统命令行参考手册》

《网络卫士防火墙系统产品说明》

《Topsec 扩展模块安装指南》

1.6 技术支持

天融信公司对于生产的安全产品提供远程的产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

1）公司主页

公司主页 www.topsec.com.cn提供交互网络服务，用户及合作伙伴可以在世界的任何地方，任何时候访问 www.topsec.com.cn技术支持中心，获取实时的网络安全解决方案、安全服务和各种安全资料。

在线技术支持

http://www.topsec.com.cn/bbs/

在线技术资料

http://www.topsec.com.cn/support/down.asp

安全解决方案

http://www.topsec.com.cn/solutions/qw.asp

2）技术支持中心

天融信公司的技术服务体系由总公司、大区技术支持中心、各省分公司、办事处、集成商、代理商等多级机构共同组成。原则上，当地的服务由当地的集成商、代理商、办事处、分公司提供；如果当地分支机构人力不足或者技术支持难度很大时，各省所在的大区技术支持中心将派出工程师协助解决；北京总部则在大区技术支持中心人力不足或者解决问题困难较大时，将直接对用户提供服务。

天融信免费安全服务热线：800-810-5119

获取技术支持中心最新联系方式，请访问：

http://www.topsec.com.cn/support/support.asp

2 安装网络卫士防火墙

本章介绍了安装防火墙前的准备工作，以及防火墙的物理安装过程，同时介绍了几种登录防火墙的方式，以便管理员对防火墙进行管理。包括如下主要内容：

- 网络卫士防火墙系统的组成与规格
- 配置网络卫士防火墙的工作模式
- 网络卫士防火墙系统的安装
- 登录并管理网络卫士防火墙
- 网络卫士防火墙的出厂配置

2.1 系统组成与规格

2.1.1 系统组成

- 网络卫士防火墙（硬件）
- 集中管理器（软件）：网络卫士防火墙专用管理软件，运行于中文 WindowsNT4.0、Windows2000/2003、WindowsXP 环境下。
- 认证客户端（软件）：网络卫士防火墙客户认证专用软件，运行于中文 WindowsNT4.0、Windows2000、WindowsXP 环境下；网络卫士防火墙 V3.3 支持以下认证：本地认证、Radius、TACACS+、LDAP、域认证、SecurID、证书认证等。
- 其他配套软件：具体请参见随机光盘的 README.TXT 描述。

2.1.2 系统规格

网络卫士防火墙不同型号产品的电源参数、环境规范、物理规格、执行标准和安全规范及标准的内容可能会有所不同，具体请参见《网络卫士防火墙系统产品说明》。

2.2 确定防火墙的工作模式

网络卫士防火墙作为一种网关型产品，通常部署在重要的安全节点或者互联网的入口处，可以通过网络设备，如交换机或 HUB，将安全区连接到网络卫士防火墙的网络接口。在安装网络卫士防火墙之前，网络管理人员可根据网络应用的实际情况以及网络中主机、服务器等设备的安全属性来规划安全区域。

在网络规划时，一般会碰到两种情况：第一种情况是在当前运行的网络中添加网络卫士防火墙。在这种情况下，网络卫士防火墙的安装环境为一个已经建立并正在运行的网络，目的通常是增强现有网络的防御能力。在此类网络中部署网络卫士防火墙，往往要求尽可能少改动或不改动网络节点的网络属性，如网络拓扑结构、网络设备地址等，并要求网络卫士防火墙的接入对网络通信造成的影响最少，尽可能地做到网络卫士防火墙部署透明。在这种环境下部署的网络卫士防火墙的工作模式最好采用透明模式。此时，网络卫士防火墙将作为二层网络设备，学习并建立 MAC 地址表，快速转发数据报文，提高转发效率。

另一种情况是在设计网络结构和部署网络设备的初始阶段，需要充分考虑网络的安全问题，并将网络卫士防火墙的安全和通信等功能融入网络设计方案。在这种情形下，网络卫士防火墙的工作模式最好设定为混合模式，即某些区域（接口）工作在透明模式下，而其他的区域（接口）工作在路由模式下。在透明模式中，可以将同一应用业务的服务器和客户机通过同一网段连接起来，以提高整体网络的通信性能。网络卫士防火墙的路由模式提供完整的静态路由功能，对于中小规模的内部网络，完全可以代替内网路由器。同时，可以启用网络卫士防火墙的通信功能，如路由、地址转换等，以便平滑地将防火墙集成到已存在的网络环境中。另外，在该工作模式下，网络卫士防火墙可以更好地支持网络扩展，如可以在对网络卫士防火墙原有的配置不作改变或只作少量修改的情况下，实现在原有网络基础上增加网段或主机。

网络卫士防火墙部署案例请参见 3配置案例。

提示

- 在网络卫士防火墙的初始缺省设置中，Eth0 接口对应着内部网络防火区。

2.3 系统安装

2.3.1 硬件设备安装

一般遵循如下步骤安装硬件设备：

1）支架安装

机架式网络卫士防火墙采用为标准 19 英寸机箱，可以安装固定在标准机柜中，随机附件中有一对上架支架(侧耳)，将其固定在网络卫士防火墙上。

2）将网络卫士防火墙置于机柜托架上

网络卫士防火墙要求放在机柜的托架上，并适当调节机柜托架与网络卫士防火墙的相对位置，使网络卫士防火墙的固定支架在垂直方向上受力较小。

3）本地一台管理主机通过 CONSOLE 线缆与网络卫士防火墙的 CONSOLE 口连接，供超级管理员进行初步配置。

4）把网络卫士防火墙的网络接口通过直通网络线与对应防火区域中的网络设备相连接。

5）通过电源线连接网络卫士防火墙和电源。

6）启动网络卫士防火墙电源（电源开关位于设备后端）。

提示

- ✧ 请确认网络卫士防火墙的防火区域与网络卫士防火墙接口名称的对应关系。
- ✧ 请注意随机配件中直通线(Passthrough)和交叉线(Crossover)的使用方法：交叉线用于通信主机间的直接连接，如网络卫士防火墙与主机间的直接连接；直通线用于网络卫士防火墙和网络设备的连接，例如网络卫士防火墙与交换机等的连接。
- ✧ 此硬件安装说明适用于机架型产品。对于桌面型产品，可以略过步骤 1）和步骤 2）。

2.3.2 管理器安装

系统最低配置：

CPU：奔腾III500

内存：128MB

显示卡：标准 VGA

硬盘：剩余空间 100MB 以上

网卡：一块 10M 局域网卡

操作系统为 Windows NT/2000 以上版本，并正确设置 TCP/IP 协议。

建议配置：

CPU：奔腾 IV 或更高

内存：256MB 或更高

显示卡：SVGA，16 位真彩以上显示模式

硬盘：剩余空间 400MB 以上

网卡：一块 100M 局域网卡

操作系统为 Windows NT/2000 以上版本，并正确设置 TCP/IP 协议。

因为网络卫士防火墙的管理主机可直接配置安全策略，所以管理主机的安全直接关系到安全系统的有效性。在网络规划中，必须谨慎设计管理主机的物理位置：要做到既确保管理的安全性，又具备管理上的方便性。通常，管理主机位于管理中心网络的网管主机上，管理中心为内部防火区的子集；同时，管理主机或管理中心与其它安全区域相比有更严格的访问安全策略。

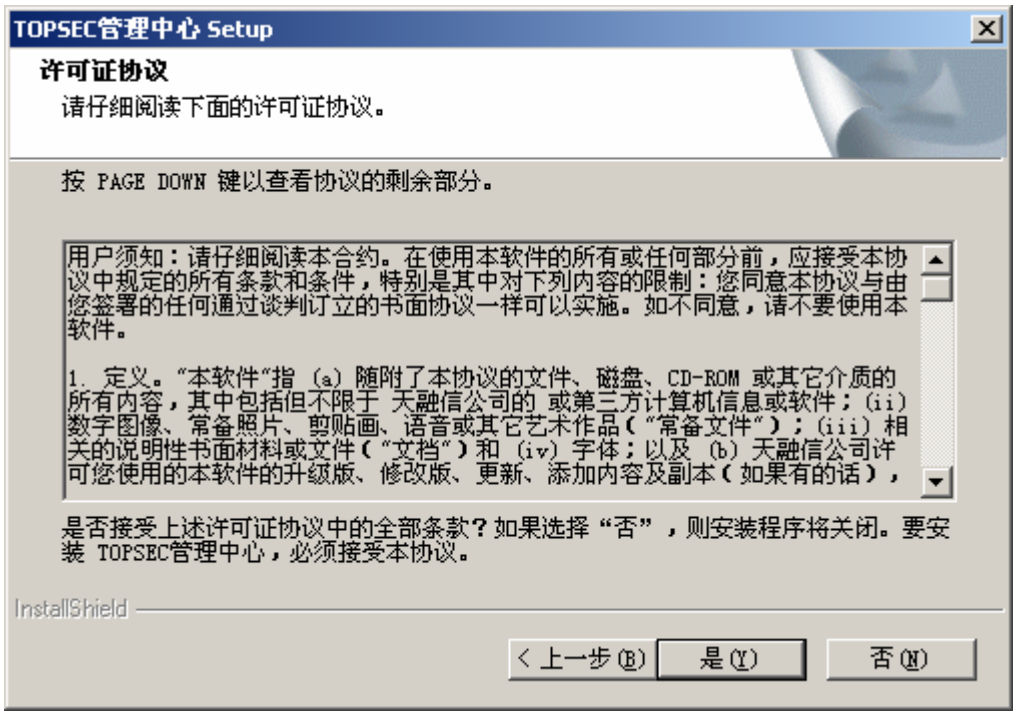
网络卫士防火墙的管理主机分本地管理主机和远程管理主机。

- **本地管理器**：可以使用任何类型的终端，如 WINDOWS 的超级终端（hypertrm.exe），终端类型至少支持 VT100 或 ANSI 等常用类型；
- **远程管理器**：为网络卫士防火墙专用的集中管理软件，弥补了通过浏览器方式管理网络卫士防火墙的功能方面的不足。

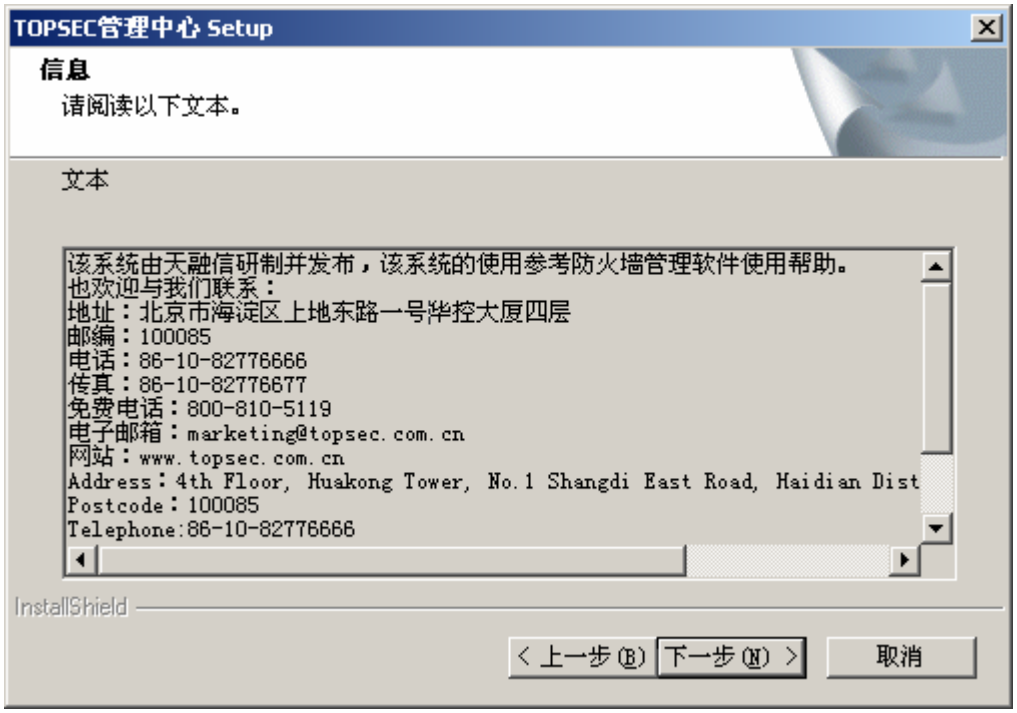
产品随机光盘内包含了安装程序，安装过程如下：

1）运行随机光盘上的集中管理器安装程序，进入安装界面。

2）按“**下一步**”按钮，进入许可证协议窗口。

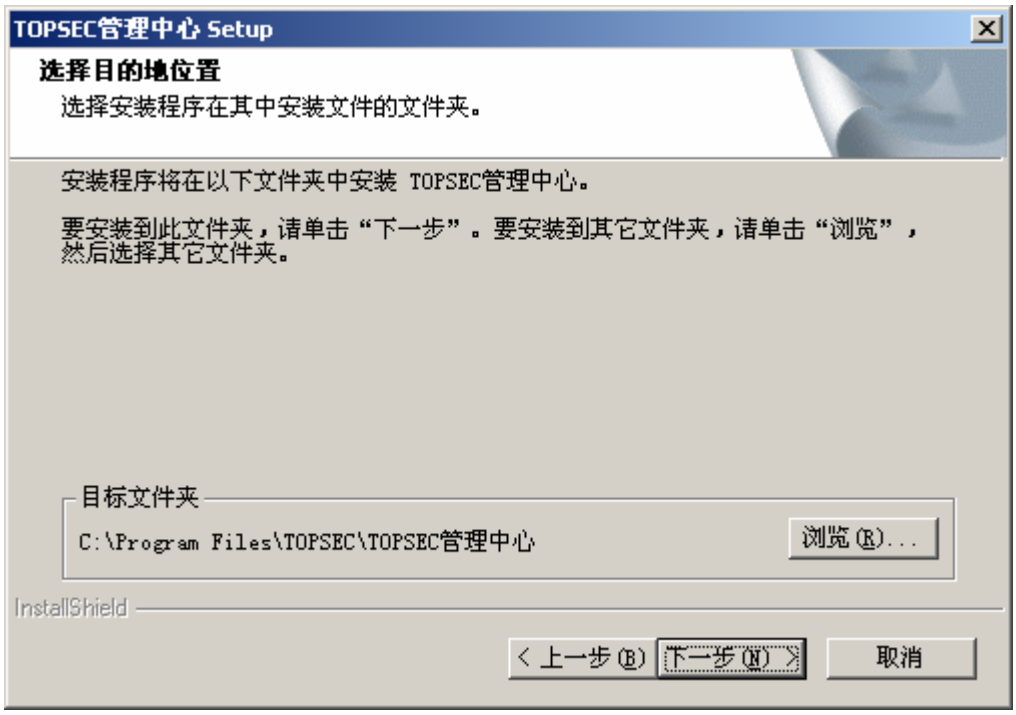


3）如果同意，按“**是**”按钮，进入信息窗口，显示关于此集中管理器的相关信息；

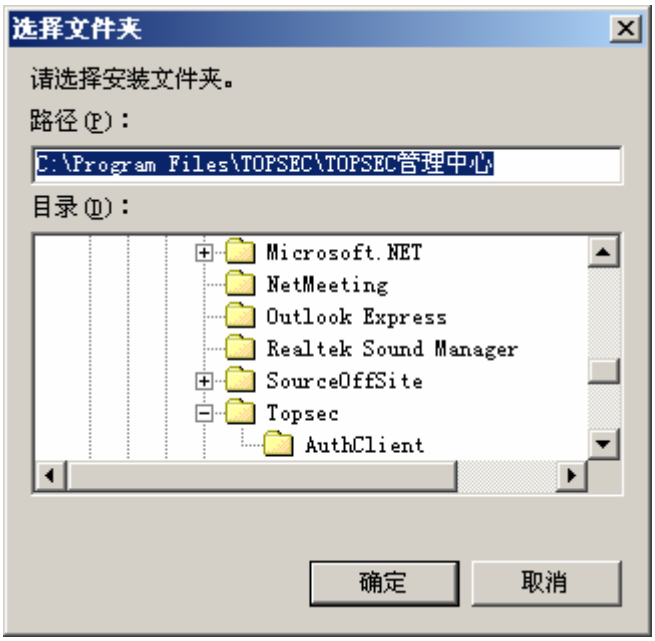


4）按“**下一步**”按钮，进入客户信息窗口。可在此窗口输入用户相关的信息；

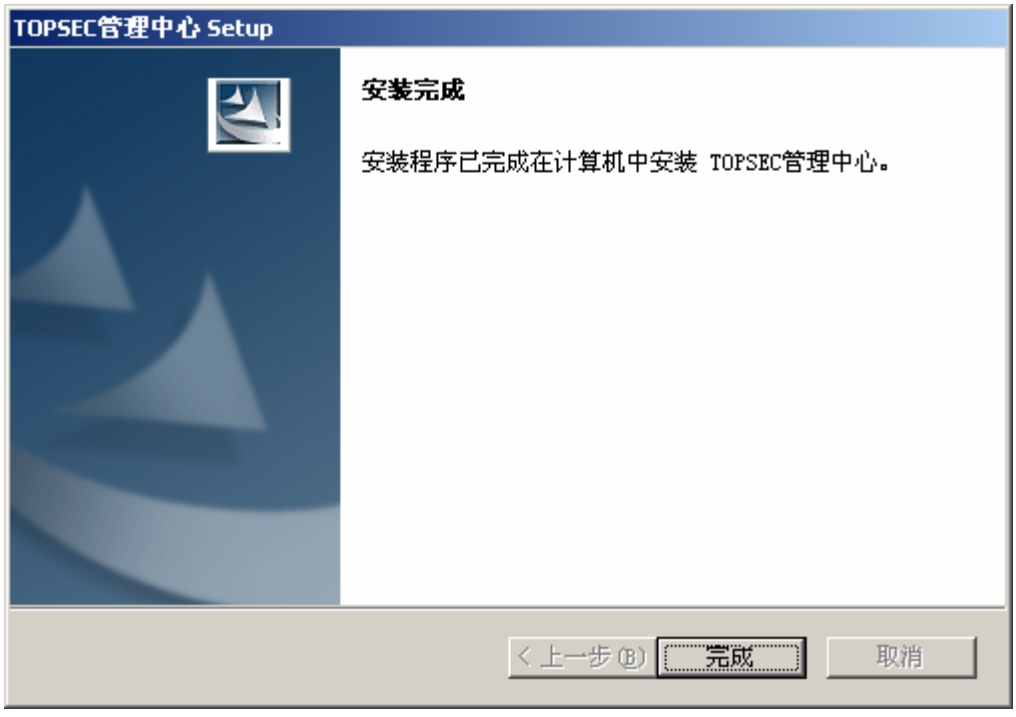
5）按“**下一步**”按钮，进入选择安装路径窗口。



6）系统默认的安装路径是当前操作系统盘符下的\Program Files\TOPSEC\TOPSEC 管理中心目录下，用户可按“**浏览**”按钮自行更改。



7）然后按“**确认**”后，返回安装界面。点击“**下一步**”按钮后，系统开始安装集中管理器软件。安装完成后，弹出如下界面，则表示安装已经完成。



2.3.3 检查网络卫士防火墙的工作状态

网络卫士防火墙的硬件设备和管理软件安装完成之后，就可以通电使用。在网络卫士防火墙的工作过程中，用户可以根据网络卫士防火墙面板上的指示灯来判断网络卫士防火墙的工作状态，具体请见下表。

指示灯名称	指示灯状态描述
工作灯	当网络卫士防火墙进入工作状态时，工作灯闪烁。
主从灯	不启用双机热备时，主从灯处于熄灭状态；在启动双机热备时，主从灯亮的时候，代表这台设备处于工作模式；反之，如果主从灯处于熄灭状态，则该网络卫士防火墙工作在备份模式。
管理灯	当网络管理员登录网络卫士防火墙时，管理灯点亮。
日志灯	当有日志记录动作发生时，且前后两次日志记录发生的时间间隔超过 1 秒钟时，日志灯会连续闪烁 4 次。

提示

✧ 某些桌面型防火墙指示灯可能会有所不同。

2.4 登录网络卫士防火墙

网络管理员可以通过多种方式管理网络卫士防火墙。管理方式包括

- 本地管理，即通过 CONSOLE 口登录网络卫士防火墙进行管理；
- 远程管理，包括使用浏览器、网络卫士防火墙集中管理器、或者通过 SSH 等多种方式登录网络卫士防火墙进行配置管理。

第一次使用网络卫士防火墙，管理员可以通过 CONSOLE 口以命令行方式、通过浏览器以 WEBUI 方式或通过 TOPSEC 管理中心进行配置和管理。在下面几节中，将会介绍如何通过 CONSOLE 口登录到网络卫士防火墙并配置其他几种管理方式。其中，WEBUI 管理方式是最方便、也是最常用到的管理方式。

2.4.1 缺省出厂配置

网络卫士防火墙在出厂时使用了以下默认配置：

管理用户	管理员用户名	superman
	管理员密码	talent 或 12345678
系统参数	设备名称	TopsecOS
	同一管理员最多允许登录失败次数	5

	最大并发管理数目 最大并发管理地点 同一用户最大登录地点 空闲超时	5 5 5 3 分钟
物理接口	Eth0（或 LAN 口） 其他接口	IP：192.168. 1.254/24 Shutdown
服务访问控制	WEBUI 管理（通过浏览器管理防火墙） GUI 管理（通过 TOPSEC 管理中心） SSH（通过 SSH 远程登录管理） 升级（对网络卫士防火墙进行升级） PING（PING 到网络卫士防火墙的接口 IP 地址或 VLAN 虚接口的 IP 地址） 其他服务	允许来自 Eth0（或 LAN 口）上的服务请求 允许来自 Eth0（或 LAN 口）上的服务请求 允许来自 Eth0（或 LAN 口）上的服务请求 允许来自 Eth0（或 LAN 口）上的服务请求 允许来自 Eth0（或 LAN 口）上的服务请求 禁止
地址对象	地址段名称 地址段范围	any 0.0.0.0 - 255.255.255.255
区域对象	区域对象名称 绑定属性 权限	area_eth0 eth0 允许
日志	日志服务器 IP 地址 日志服务器开放的日志服务端口	IP：192.168. 1.253 UDP 的 514 端口
高可用性（HA）		关闭

2.4.2 使用 CONSOLE 口登录网络卫士防火墙

通过 CONSOLE 口登录到网络卫士防火墙，可以使用命令行方式对网络卫士防火墙进行一些基本的设置，用户在初次使用网络卫士防火墙时，通常都会登录到网络卫士防火墙更改防火墙的出厂配置（更改接口 IP 地址等），以便在不改变现有网络结构的情况下将网络卫士防火墙接入网络中。这里将详细介绍如何通过 CONSOLE 口连接到网络卫士防火墙。

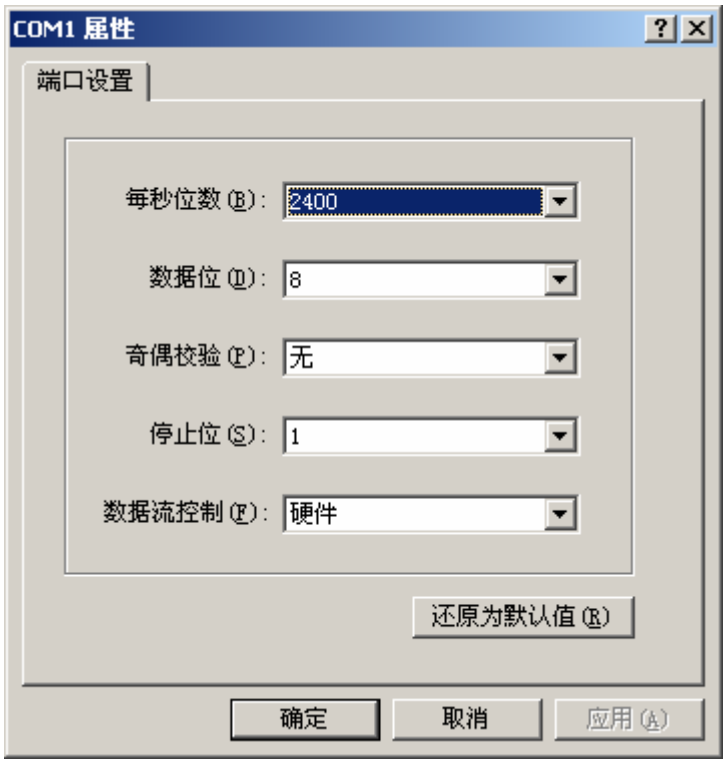
1）将 CONSOLE 口控制线（扁平象牙白色）的 RJ45 接口端和网络卫士防火墙的 CONSOLE 口相连接，DB-9 接口端和计算机的串口（这里假设使用 COM1）相连接。（部分产品无 RJ45 接口形式的 Console 口，故需要使用 DB9-DB9 Console 控制线）

2)在计算机中建立网络卫士防火墙和管理主机的连接。

选择 **开始 > 程序 > 附件 > 通讯 > 超级终端**，系统提示输入新建连接的名称。如下图所示。

用户可以输入任何名称，这里假设名称为 topsec，输入名称确定后，提示选择使用的接口（假设使用 COM1），如下图所示。

点击“确定”按钮后，可以对 COM1 的属性进行设置，如下图所示。



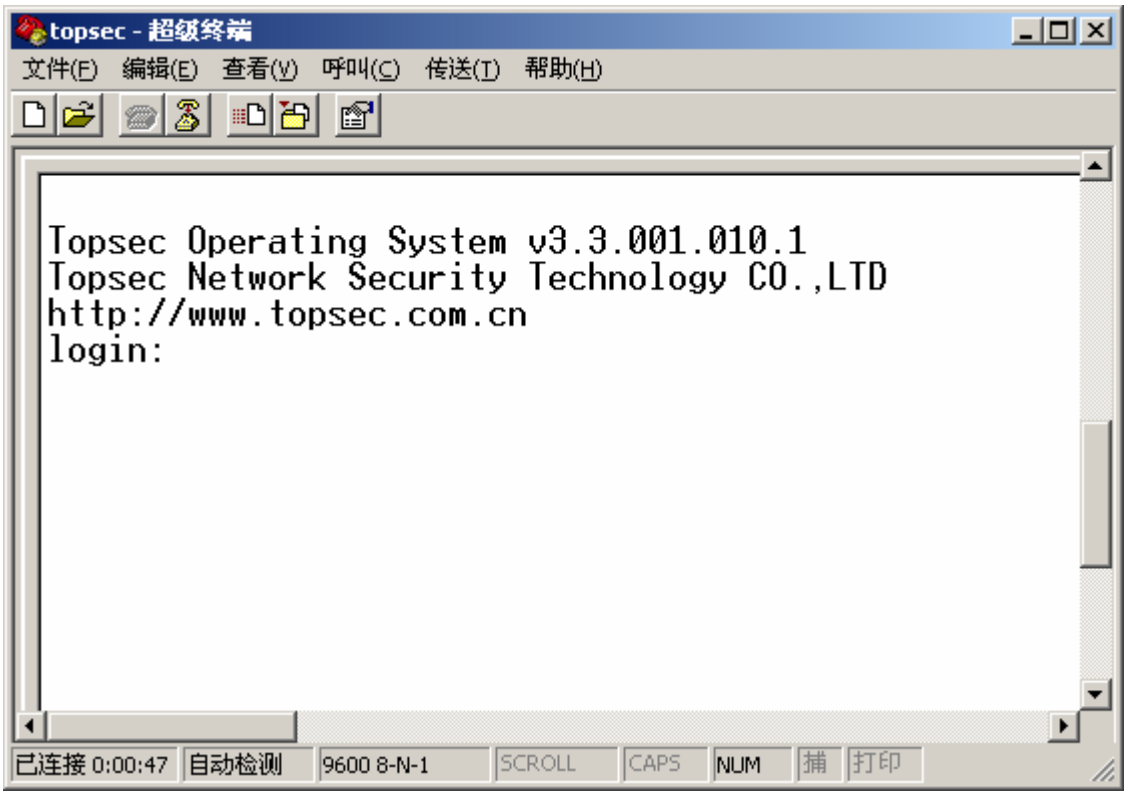
用户可以点击“还原为默认值”按钮，也可以按照以下参数设置 COM1 口的属性。

每秒位数：	9600
数据位：	8
奇偶校验：	无
停止位：	1
数据流控制：	无

提示

- ✧ TG-4207、TG-1607、TG-1607-VPN、TG-1507、TG-1507-VPN、TG-1503、TG-1503-VPN、TG-1403-VPN、TG-1405-VPN、TG-1305-VPN 产品使用 115200bps 的连接速率。

成功连接到网络卫士防火墙后，超级终端界面会出现输入用户名和密码提示，如下图所示。



用户直接输入网络卫士防火墙默认的串口登录用户：**superman** 和密码：**talent**（由于有些设备被抽样检测，所以有些设备的缺省密码被修改为“12345678”），即可登录到网络卫士防火墙。

3）登录后，用户就可使用命令行方式对网络卫士防火墙进行配置管理等操作。

提示

- ✧ 网络卫士防火墙对于用户名和密码大小写敏感；
- ✧ 本地管理员具有网络卫士防火墙所有管理权限，为超级管理员；
- ✧ 关于如何通过命令行配置网络卫士防火墙，请参考《网络卫士防火墙系统命令行参考手册》。

2.4.3 设置其他管理方式

从 CONSOLE 口本地登录网络卫士防火墙后，管理员可以通过命令行对防火墙进行一些必要的设置，如更改、添加接口 IP，添加其他的远程管理方式（包括“WEBUI 管理”、“SSH”等），方便对网络卫士防火墙的管理维护。

本节将介绍如何使用命令行方式添加其它管理方式。另外，管理员还可以使用浏览器通过 Eth0 接口对防火墙进行设置，这要求管理主机与 Eth0 的缺省出厂 IP 处于同一网段。

2.4.3.1设置接口 IP 地址

用户可通过网络卫士防火墙的任一物理接口远程管理网络卫士防火墙，但是在此之前，管理员必须为此物理接口配置 IP 地址，作为远程管理网络卫士防火墙的管理地址。命令行语法如下：

network interface〈*string*〉**ip add**〈*ipaddress*〉**mask**〈*netmask*〉

参数说明：

string：网络卫士防火墙物理接口名称，字符串，例如 *eth0*。

ipaddress：IP 地址，如 *192.168.91.22*。

netmask：子网掩码，如 *255.255.255.0*。

2.4.3.2定义地址对象

管理员应定义允许远程管理网络卫士防火墙的 IP 地址范围，可以是某一特定的 IP 地址，也可以来自某一子网或地址范围。在命令行中使用 **define host/define subnet/define range** 这几个命令定义 IP 地址、子网或地址范围。命令行语法如下：

定义 IP：**define host add name**〈*string*〉**ipaddr**〈*ipaddress*〉

定义子网：**define subnet add name**〈*string*〉**ipaddr**〈*ipaddress*〉**mask**〈*netmask*〉

定义地址范围：**define range add name**〈*string*〉**ip1**〈*ipaddress*〉**ip2**〈*ipaddress*〉

参数说明：

string：对象名称，字符串。

ipaddress：IP 地址，如 *192.168.91.22*。

netmask：子网掩码，如 *255.255.255.0*。

成功定义后系统会自动为已定义的 IP 地址、子网或地址范围生成对应的 ID 号。查看用户已定义的对象的 ID 号命令行语法如下：

查看已定义的所有 IP 地址对象：**define host show**

查看已定义的所有子网对象：**define subnet show**

查看已定义的所有地址范围对象：**define range show**

2.4.3.3指定管理方式

管理员可以为已定义的 IP 地址（或子网、地址段）指定其可使用的远程管理方式。在命令行中可以使用 pf service 命令指定管理方式。命令行格式如下：

pf service add name 〈gui|snmp|ssh|monitor|ping|telnet|tosids|pluto |auth|ntp|update |otp|dhcp|rip|l2tp|pptp|webui|vrc|vdc〉 **area** 〈*string*〉〈[**addressid** 〈*number*〉]｜［**addressname** 〈*string*〉]〉［**vsid** <*number*>］

相关参数说明：

参数	说明
add	增加一条服务访问规则
name	选择 TOS 设备开放的服务名
gui	通过图形界面访问设备
snmp	开放 SNMP 服务
ssh	开放 SSH 服务
monitor	开放监控服务
ping	开放 PING 服务
telnet	通过 TELNET 访问设备
tosids	开放 IDS 服务
pluto	开放 IKE 服务
auth	开放认证服务
ntp	开放 NTP 服务
update	开放升级防火墙的服务
otp	开放 OTP 服务
dhcp	开放动态主机配置服务
rip	开放 RIP 服务
l2tp	开放 L2TP 服务
pptp	开放 PPTP 服务
webui	开放通过 WEBUI 管理网络卫士防火墙的服务
vrc	VRC 服务
vdc	开放接收 SPS 的反向通告端口、及向 SPS 发送通告的源端口，使用 UDP 协议的 2010 端口
area	选择允许服务请求来自哪个区域，只能从现有区域中选择一个
string	网络卫士防火墙网络区域名称（字符串）
addressid	设定允许客户地址对象 ID 号
number	数值，必须是已经定义的主机、子网或范围地址对象的 ID 号
addressname	设定允许客户地址对象名称
string	字符串，必须是已经定义的主机、子网或范围地址对象名
vsid	该服务访问规则所属的虚系统 ID 号
number	数值，范围为 0-255；默认为 0，表示不属于任何虚系统

2.4.3.4设置管理方式实例

下面是个简单的配置实例，用以说明如何设置网络卫士防火墙的 WebUI 管理方式：

1．为网络卫士防火墙的物理接口 Eth1 配置 IP 地址 192.168.91.88，子网掩码是 255.255.255.0，此地址将作为网络卫士防火墙的管理地址：

进入 network 组件	topsecos# network
配置 Eth1 接口 IP	topsecos.network# interface eth1 ip add 192.168.91.88 mask 255.255.255.0

2．定义一个 area 对象“webui-area”，并设置其属性为 eth1：

进入 define 组件	topsecos.network# exit topsecos# define
配置 Eth1 接口 IP	topsecos.define# area add name webui-area attribute eth1 access on

3．定义一个 IP 地址对象“manage-host”，地址是 192.168.91.250，此地址是被允许的远程管理网络卫士防火墙的地址：

保持 define 组件	topsecos.define#
定义管理主机对象	topsecos.define# host add name manage-host ipaddr 192.168.91.250

4. 设置从 192.168.91.250 这个 IP 可以浏览器远程管理该防火墙:

进入 pf 组件	topsecos.define# exit topsecos# pf
定义管理主机对象	topsecos.pf# service add name webui area webui-area addressname manage-host

2.4.4 管理主机的相关设置

在网络卫士防火墙上成功添加管理方式后，还需要在管理主机进行必要设置才能远程管理防火墙。下面简要说明了不同管理方式的管理主机的要求：

SSH，需要 SSH 软件，如 PUTTY 等，需要设置连接地址为网络卫士防火墙管理地址；

WEBUI，需要在管理主机安装浏览器，并进行必要的配置。

提示

- ✧ 管理主机的浏览器需支持 SSLv2.0、SSLv3.0 或 TLSv1.0 协议中的任意一种。
- ✧ 网络卫士防火墙支持 IE5.0，IE6.0，Mozilla firefox 1.0.2，Mozilla firefox1.0.3，Mozilla Firefox 1.0.4，Mozilla firefox 1.0.5，Netscape7.1（只能在 Linux9.0 中支持），Netscape8.0（支持 Linux9.和 Linux10.0），Opera8.0（只支持 Windows2000 Professional, Windows2000 Server）。
- ✧ 使用前需确认浏览器选项中 cookie 相关选项打开。

2.4.5 通过浏览器登录防火墙

管理员在管理主机的浏览器上输入防火墙的管理 URL，例如：https://192.168.1.254，弹出如下的登录页面。

输入用户名密码后（网络卫士防火墙默认出厂用户名为：superman，密码为：talent 或 12345678），点击“提交”，就可以进入管理页面。

提示

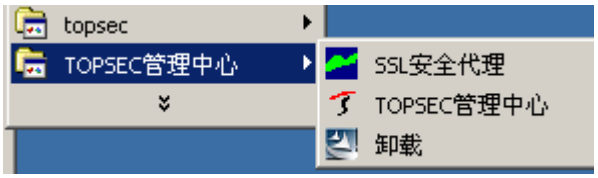
- ✧ 在输入 URL 时要注意以“https://”作为协议类型，例如 https://192.168.1.254。
- ✧ 网络卫士防火墙对于用户名和密码大小写敏感。

2.4.6 使用集中管理器登录防火墙

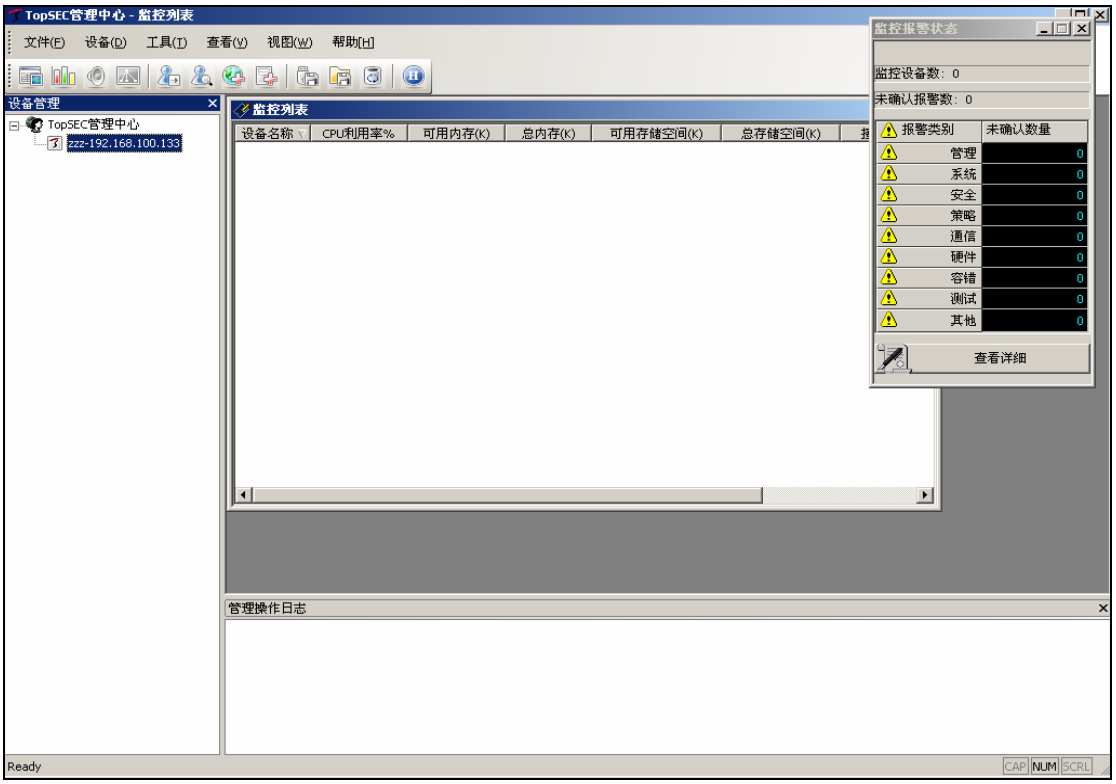
网络卫士防火墙集中管理器给用户提供了一种方便、安全的工具来远程配置和管理网络卫士防火墙。在集中管理器中，用户可以通过友好的图形界面来完成所有功能选项的配置。同时，由于管理器与网络卫士防火墙的通信是由 SSL 机制进行加密保护的，用户不必担心安全信息的泄漏问题。所以，我们推荐用户使用集中管理器来管理和配置网络卫士防火墙。

- ➢ 使用快捷菜单

管理器安装完成后，在系统启动菜单中建立了快捷菜单，如下所示：



可以直接从此处运行，以下为一运行示例：

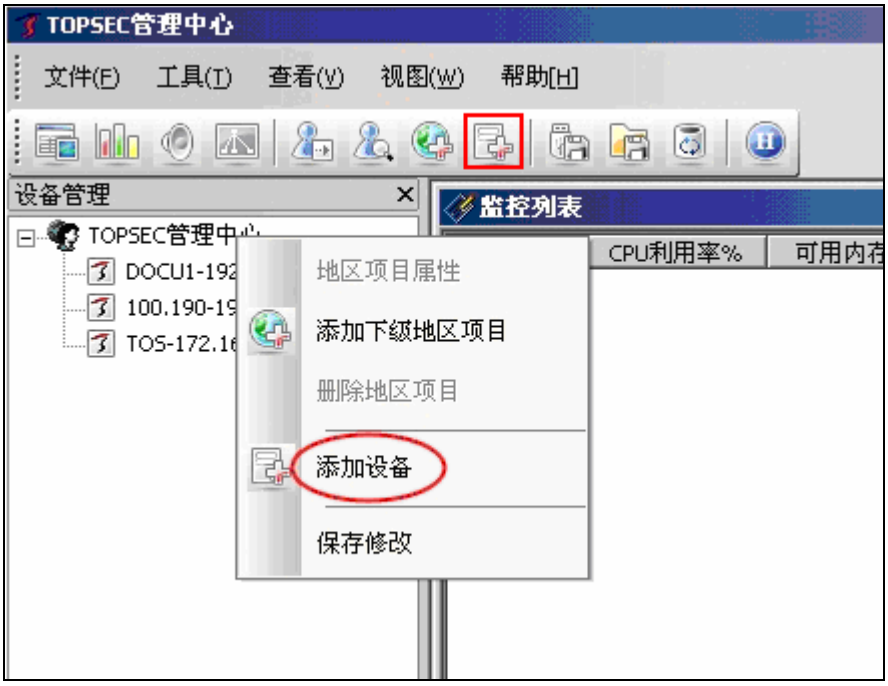


➢ 登录网络卫士防火墙

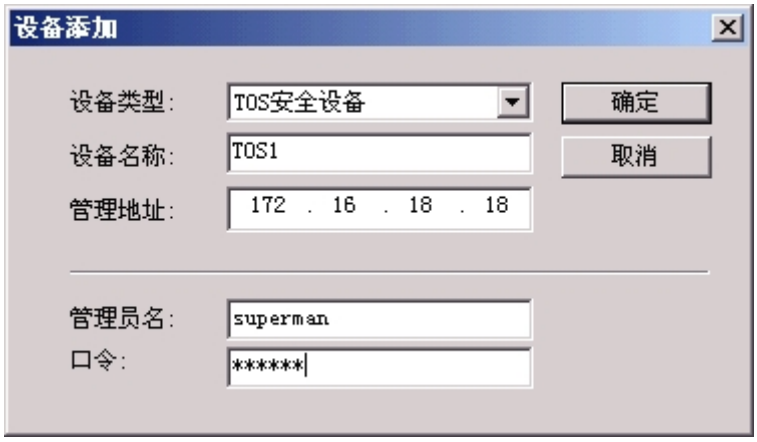
如果管理员希望通过集中管理器远程连接网络卫士防火墙，应先确定是否更改网络卫士防火墙的出厂配置。如果不更改出厂配置的话，需要把安装网络卫士防火墙集中管理器的计算机与网络卫士防火墙接口 Eth0（或 LAN 口）设在同一个网段。Eth0（或 LAN 口）接口的出厂 IP 设置为：192.168.1.254/24。

如果要更改网络卫士防火墙的出厂配置，则需要使用 CONSOLE 口控制线或交叉线连接到网络卫士防火墙，用超级终端登录到网络卫士防火墙，使用命令行方式更改网络卫士防火墙的接口地址。具体配置命令请参考《网络卫士防火墙系统命令行参考手册》。

从管理主机启动菜单运行集中管理器，管理软件启动后可以读入预定义项目。要添加一个管理项目，在 TOPSEC 管理中心设备管理窗口中点击右键，在弹出菜单中选择“**添加设备**”，也可以在管理器窗口中点击“ ”图标。



打开管理配置窗口：添加网络卫士防火墙到管理配置中：



选中新添加的网络卫士防火墙，双击它或使用右键菜单对目标防火墙进行管理或监控。具体操作方法请参见《TOPSEC 管理中心使用手册》。

2.4.7 通过 SSH 方式登录网络卫士防火墙

SSH 提供了一种更安全的机制来供用户远程管理网络卫士防火墙。在 SSH 连接中，所有的数据都是经过加密后传输，这就保证了网络卫士防火墙的关键信息，如密码等，在传输过程中不会被窃听而导致泄露。

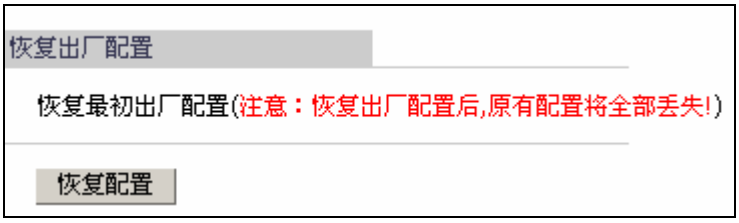
用户可以在本地主机上使用支持 SSH 的客户端软件，如用于 UNIX 系统的 OpenSSH，或用于 32 位 WINDOWS 平台的 PUTTY， 来登录网络卫士防火墙。

2.5 恢复出厂配置

系统除了提供上节所述的设备配置维护功能外，还提供了恢复出厂默认配置的功能，以方便用户重新配置设备。恢复出厂配置后，设备的网络接口地址可能会改变，配置信息会被清除，进而导致失去连接，请用户提前做好准备。

恢复出厂配置的具体操作方法如下：

1）通过浏览器登录网络卫士防火墙后，选择 **系统管理 > 维护**，点击“恢复”页签，出现如下页面。



2）点击“恢复配置”按钮，经用户确认后，系统恢复出厂配置并自动重启，此时用户与 TOS 设备的连接断开。

3 配置案例

为了更好地指导用户配置使用网络卫士防火墙，本章列举了 3 个典型案例，并详细介绍了配置过程。三个案例之间具有相互呼应的关系，具体描述如下：

- 案例 1：路由模式下通过专线访问外网，主要描述总公司接入网络卫士防火墙后的简单配置，总公司的网络卫士防火墙工作在路由模式下。
- 案例 2：混合模式下通过 ADSL 拨号访问外网，主要描述分公司网络卫士防火墙的配置，分公司的网络卫士防火墙工作在混合模式下。值得注意的是，分公司是通过 ADSL 拨号与外网进行连接的。
- 案例 3：建立 VPN 隧道，主要介绍在如上所述的网络环境中，如何在总公司与分公司之间建立 IPSec VPN 隧道。

提示

✧ 本节所举范例基于网络卫士防火墙 TopGuard 4000 系列，对于某些低端网络卫士防火墙，接口采用 LAN 或者 WAN 表示方式。一般来说，WAN 为外网接口，LAN 为内网接口。

3.1 案例 1：路由模式下通过专线访问外网

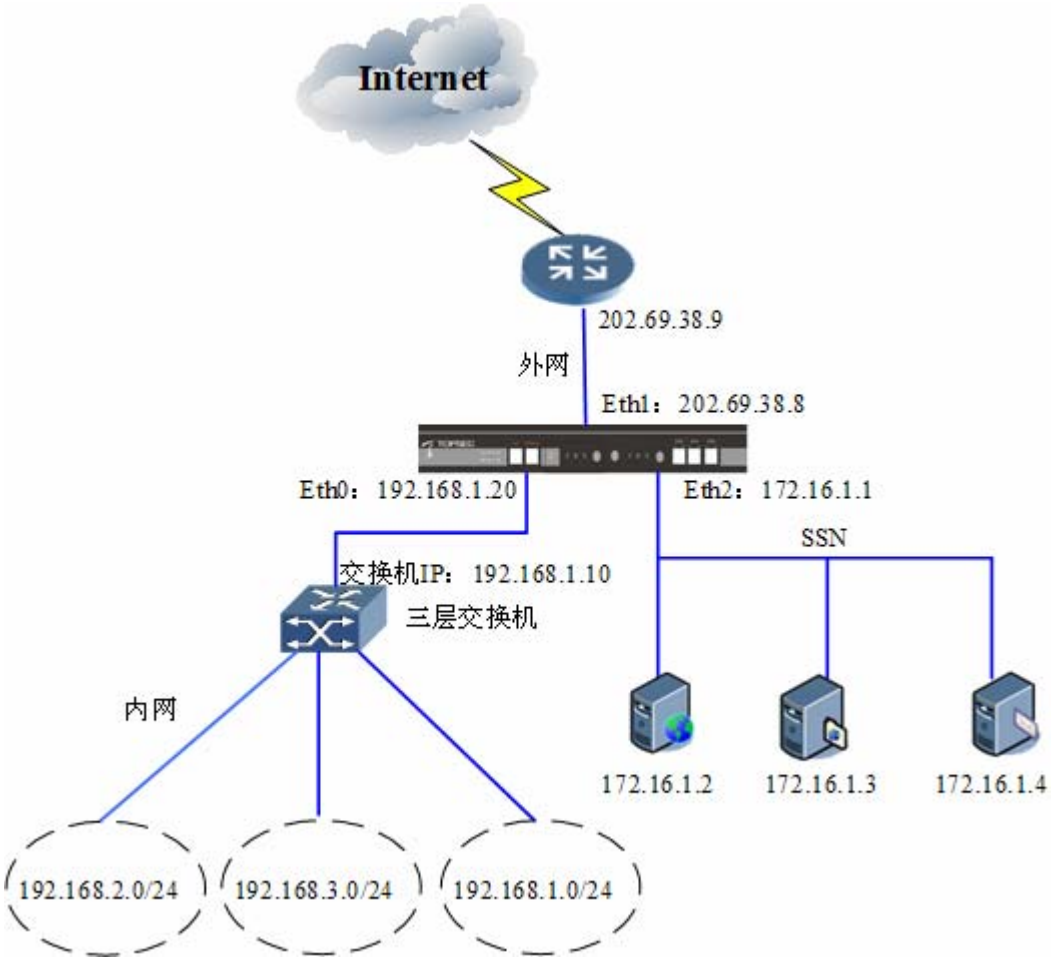


图 3-1 网络卫士防火墙的路由模式

网络状况：

- 总公司的网络卫士防火墙工作在路由模式。Eth1 属于外网区域，IP 为 202.69.38.8；Eth2 属于 SSN 区域，IP 为 172.16.1.1；Eth0 属于内网区域，IP 为 192.168.1.20。
- 网络划分为三个区域：外网、内网和 SSN。管理员位于内网中。内网中存在 3 个子网，分别为 192.168.1.0/24，192.168.2.0/24，192.168.3.0/24。
- 在 SSN 中有三台服务器，一台是 HTTP 服务器（IP 地址：172.16.1.2），一台是 FTP 服务器（IP 地址：172.16.1.3），一台是邮件服务器（IP 地址：172.16.1.4）。

用户需求：

- 内网的机器可以任意访问外网，也可访问 SSN 中的邮件服务器和 FTP 服务器；
- 外网和 SSN 的机器不能访问内网；
- 允许外网主机访问 SSN 的 HTTP 服务器。

配置步骤：

1） 为网络卫士防火墙的物理接口配置 IP 地址。

进入 NETWORK 组件	topsecos# network
配置 Eth0 接口 IP	topsecos.network# interface eth0 ip add 192.168.1.20 mask 255.255.255.0
配置 Eth1 接口 IP	topsecos.network# interface eth1 ip add 202.69.38.8 mask 255.255.255.0
配置 Eth2 接口 IP	topsecos.network# interface eth2 ip add 172.16.1.1 mask 5.255.255.0

2）内网中管理员通过浏览器登录网络卫士防火墙，设置为区域对象绑定属性，设置权限。

设置内网	绑定属性为“Eth0”，权限选择为禁止
设置外网	绑定属性为“Eth1”，权限选择为允许
设置 SSN	绑定属性为“Eth2”，权限选择为禁止

3)定义地址对象

定义 HTTP 服务器	主机名称设为 HTTP_SERVER，IP 为 172.16.1.2
定义 FTP 服务器	主机名称设为 FTP_SERVER，IP 为 172.16.1.3
定义邮件服务器	主机名称设为 MAIL_SERVER，IP 为 172.16.1.4
定义虚拟 HTTP 服务器	主机名称设为 V_SERVER，IP 为 202.69.38.10

4)定义访问规则

允许内网用户访问 HTTP 服务器	源区域选择“内网” 目的区域选择“SSN”，目的地址选择“HTTP_SERVER” 服务选择“HTTP” 访问权限选择“允许”，并启用该规则
允许内网用户访问邮件服务器	源区域选择“内网” 目的区域选择“SSN”，目的地址选择“MAIL_SERVER” 服务选择“POP3”，“SMTP” 访问权限选择“允许”，并启用该规则
允许内网用户访问 FTP 服务器	源区域选择“内网” 目的区域选择“SSN”，目的地址选择“FTP_SERVER” 服务选择“FTP” 访问权限选择“允许”，并启用该规则
允许外网用户访问 HTTP 服务器	源区域选择“外网” 目的区域选择“SSN”，目的地址选择“HTTP_SERVER” 服务选择“HTTP” 访问权限选择“允许”，并启用该规则

5)定义地址转换规则

内网用户通过源地址转换访问外网	转换控制选择“SNAT” 源区域选择“内网” 目的区域选择“外网” 服务不选，表示全部服务 源地址转换为“Eth1”
外网用户通过目的地址转换访问 HTTP 服务器	转换控制选择“DNAT” 源区域选择“外网” 目的区域选择“SSN”，目的地址选择“V_SERVER” 服务选择“HTTP” 目的地址转换为“HTTP_SERVER”

6）定义路由

为内网用户访问 Internet 添加缺省路由	目的地址设为“0.0.0.0” 网关地址设为“202.69.38.9”
添加回指路由，为发往内网的数据包指定路由	目的地址设为“192.168.0.0” 网关地址设为“192.168.1.10”

3.2 案例 2：混合模式下通过 ADSL 拨号访问外网

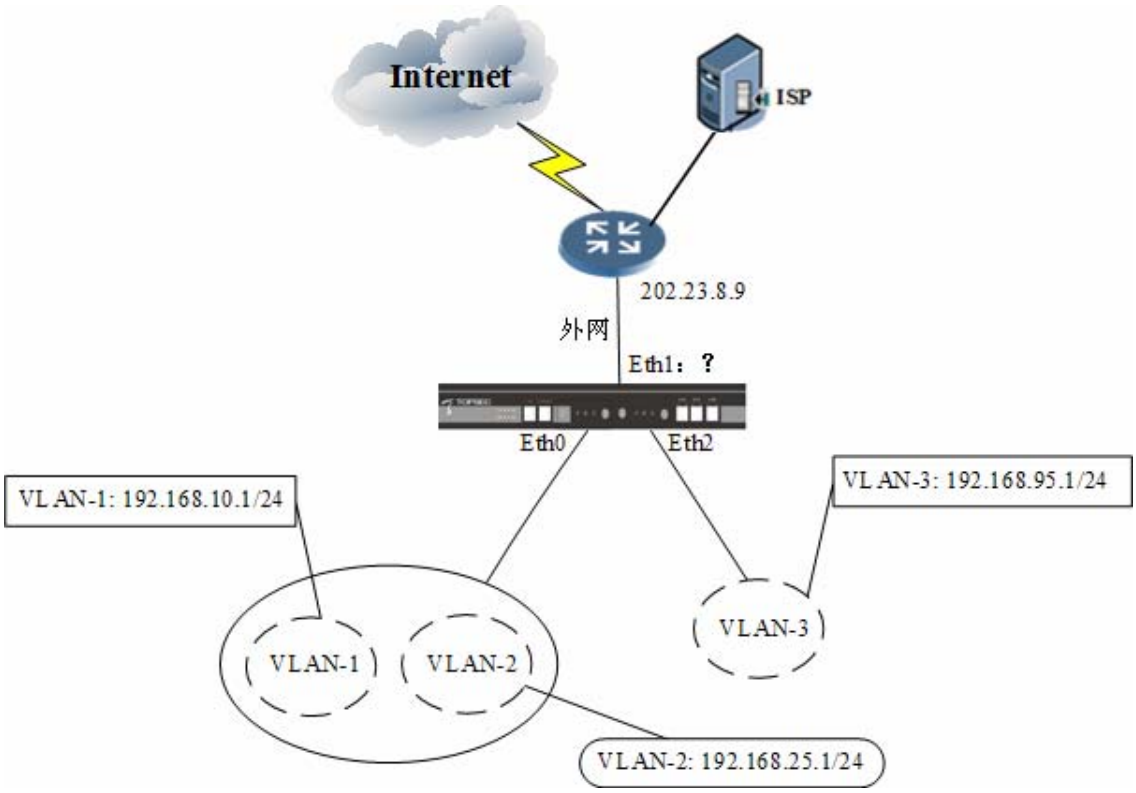


图 3-2 网络卫士防火墙的混合模式

网络状况：

- 分公司的网络卫士防火墙工作在混合模式。

  Eth1 为路由接口，属于外网区域，通过路由器与外部网络及 ISP 相连（该接口由 ADSL 拨号获取公网 IP）；

  Eth0 和 Eth2 均为交换接口，Eth0 工作在 Trunk 方式下，Eth2 工作在 Access 方式下；

  Eth0 下连接着 2 个 VLAN，VLAN-1 和 VLAN-2；

  Eth3 下连接着 1 个 VLAN，VLAN-3。

- VLAN-1 的 IP 为 192.168.10.1/24；

  VLAN-2 的 IP 为 192.168.25.1/24；

  VLAN-3 的 IP 为 192.168.95.1/24。

- 管理主机位于 VLAN-1 内。

用户需求：

- 防火墙通过 ADSL 拨号获取 Eth1 的公网 IP 地址。
- VLAN-1 内的机器可以任意访问外网（NAT 方式）， VLAN-2 和 VLAN-3 内的机器禁止访问外网。
- 外网的机器不能访问 VLAN-1 与 VLAN-2；外网的机器可以访问 VLAN-3。

配置步骤：

1）通过 CONSOLE 口登录网络卫士防火墙，配置基本信息。

进入 network 组件	topsecos # **network**
添加 VLAN-1	topsecos.network# vlan add id 0001
配置 VLAN-1 的管理 IP	topsecos.network# interface vlan.0001 ip add 192.168.10.1 mask 255.255.255.0
配置 Eth0 接口为交换接口	topsecos.network# interface eth0 switchport mode trunk
设置 Eth0 接口控制的 VLAN	topsecos.network# interface eth0 switchport trunk allowed-vlan 0001，0002

2）管理员通过 VLAN-1 的管理 IP 登录网络卫士防火墙，并绑定 Eth1 口和 ADSL 的拨号属性、设置区域对象及 VLAN。

设置区域（外网）	绑定属性为“adsl”； 权限设为允许访问。
添加 VLAN-2	管理 IP 设为“192.168.25.1”，MASK 设为“255.255.255.0”。

添加 VLAN-3	管理 IP 设为“192.168.95.1”，MASK 设为“255.255.255.0”。

3）设置接口

设置接口 Eth2	设置为“交换接口”； 接口类型为“access”； VLAN 范围为“3”。

4）设置 ADSL 拨号参数

设置 ADSL 拨号参数	接口设置为“Eth1”； 用户名和密码根据 ISP 服务商提供的参数值进行设置； 绑定属性为“adsl”。

5）定义访问规则

禁止 VLAN-2 用户访问外网	源 VLAN 选择“VLAN 0002”； 目的区域选择“外网”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则。
禁止 VLAN-3 用户访问外网	源 VLAN 选择“VLAN 0003”； 目的区域选择“外网”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则。
禁止外网用户访问 VLAN-1	源区域选择“外网”； 目的 VLAN 选择“VLAN 0001”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则。
禁止外网用户访问 VLAN-2	源区域选择“外网”； 目的 VLAN 选择“VLAN 0002”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则。

6）定义地址转换规则

VLAN-1 用户通过源地址转换访问外网	转换控制选择“SNAT”； 源 VLAN 选择“VLAN 0001”； 目的区域选择“外网”； 服务不选，表示全部服务； 源地址转换为“adsl”。

7）拨号

在防火墙上通过选择 **网络管理 > 网络链路 > ADSL** 菜单，并点击“开始拨号”按钮进行 ADSL 拨号。建立 ADSL 连接成功后，在防火墙的路由表中会增加一条内网用户访问 Internet 的路由信息：

源为“0.0.0.0/0”；

目的为“0.0.0.0/0”；

网关地址为 ISP 分配的公网 IP 地址（如：169.254.125.124）；

接口为与 Eth1 口绑定的 ppp0 口（拨号成功后，系统自动创建了一个 ppp0 口）。

3.3 案例 3：建立 VPN 隧道

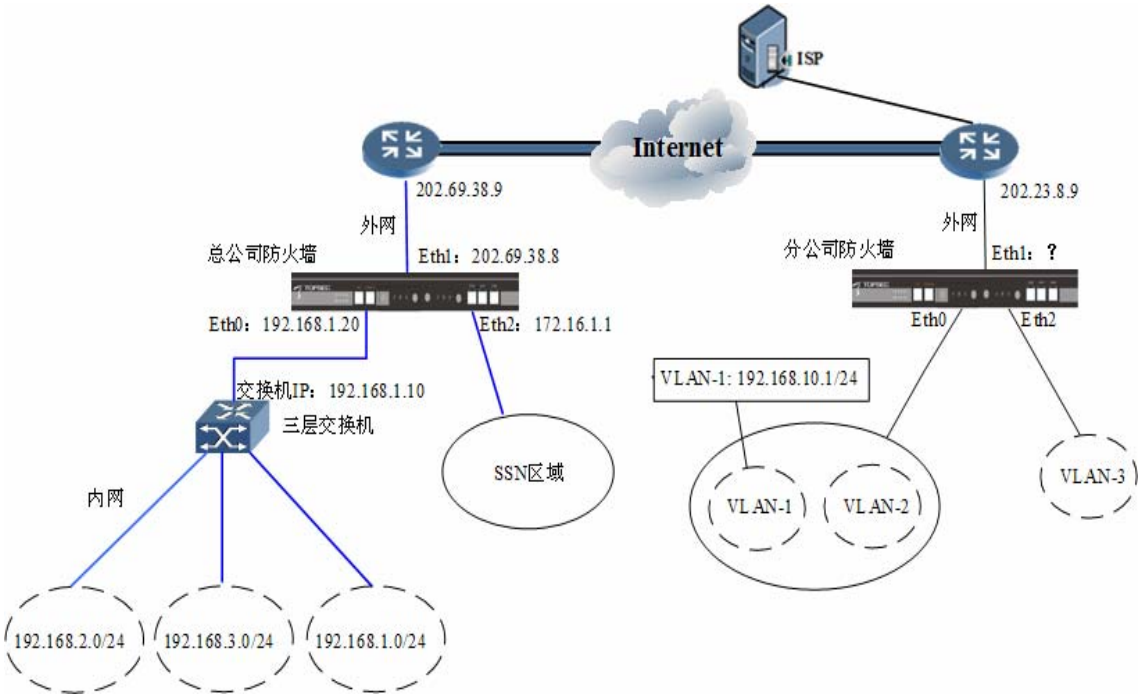


图 3-3 网络卫士防火墙的 VPN 隧道模式

网络状况：

- 总公司防火墙工作在路由模式下，接口 Eth1（IP：202.69.38.8）通过路由器与 Internet 相连；分公司防火墙工作在混合模式下，接口 Eth1 通过路由器与 Internet 相连，且 Eth1 口通过 ADSL 拨号获取公网 IP。
- 总公司防火墙的 Eth0 口与 Eth2 口分别连接公司内网区和 SSN 区域，内网区有三个子网：192.168.2.0/24、192.168.3.0/24、192.168.1.0/24。
- 分公司防火墙的 Eth0 口与 Eth2 口分别连接内网的三个 Vlan：VLAN-1、VLAN-2 和 VLAN-3，其中 VLAN-1 的 IP 为 192.168.10.1/24。

用户需求：

- 分公司的 VLAN-1 所在子网 192.168.10.0/24 与总公司子网 192.168.2.0/24 之间建立基于预共享密钥认证的 VPN 通信。

配置步骤：

1）配置总公司防火墙，具体的配置步骤请参见 案例 1。

2）配置分公司防火墙，具体的配置步骤请参见 案例 2。

下面只描述与建立 VPN 隧道有关的操作。

3）在总公司防火墙上开放“pluto”服务

开放 pluto 服务	服务名称为“pluto”； 控制区域为“area_eth1”； 控制地址为“any”。

4）在分公司防火墙上开放服务

开放 pluto 服务	服务名称为“pluto”； 控制区域为“area_eth1”； 控制地址为“any”。

5）在总公司防火墙上绑定虚接口

绑定虚接口	虚接口名为“ipsec0”； 绑定接口名为“eth1”； 接口地址为“202.69.38.8”。

6）在分公司防火墙上绑定虚接口

绑定虚接口	虚接口名为“ipsec0”； 绑定接口名为“eth1”； 接口地址为“0.0.0.0”。

7）在总公司防火墙上添加静态隧道，隧道参数采用默认设置。

添加静态隧道	隧道名：zong-fen IKE 协商模式：主模式 认证方式 = 预共享密钥，密钥 = as34Kui() 本地标识：@202_8 对方标识：@0_0 对方地址：0.0.0.0 本地子网：192.168.2.0

	本地掩码：255.255.255.0 对方子网：192.168.10.0 对方掩码：255.255.255.0 主动发起协商：是

8）在分公司防火墙上添加静态隧道，隧道参数采用默认设置。

添加静态隧道	隧道名：fen-zong IKE 协商模式：主模式 认证方式 = 预共享密钥，密钥 = as34Kui() 本地标识：@0_0 对方标识：@202_8 对方地址：202.69.38.8 本地子网：192.168.10.0 本地掩码：255.255.255.0 对方子网：192.168.2.0 对方掩码：255.255.255.0 主动发起协商：是

提示

- ✧ 在案例配置中未涉及的参数均采用系统缺省设置。在实际应用中请根据具体网络情况和需求进行修改。
- ✧ 本案例中分公司防火墙采用的是 ADSL 拨号的方式，故其 IP 设置为 0.0.0.0。如果建立隧道的两台防火墙均为 ADSL 环境，则可以通过 DDNS 方式，利用域名来建立隧道。关于 DDNS 的具体使用请参考用户手册的相关章节。

附录 A 扩展模块

网络卫士防火墙上安装的扩展模块包括：百兆接口扩展模块、标准千兆模块和专用千兆模块。

1．百兆接口扩展模块

百兆接口扩展模块用于网络安全产品快速以太网接口扩展，扩展的网络接口与防火墙系统配置的网络接口具有相同的性能指标和参数。支持的模块型号及接口标准如下所示。

模块型号	接口标准	适用产品型号
TopSEC-FWM-2	10/100BASE-T	百兆系列防火墙、VPN、网络密码机产品 (如 TG-4324, TV-6324, SJW11-A, TV-6424-SSL100)
TopSEC-FWME-2	10/100BASE-T	百兆高端系列防火墙、VPN、网络密码机产品 (如 TG-4424, TV-6624, SJW11-A-E, TV-6624-SSL300, TG-324-UTM, TG-4508)

2．标准千兆模块

网络卫士防火墙适用的标准千兆模块遵循 GBIC 规范 5.5 版本和 SFP MSA，可以安装在网络卫士防火墙扩展槽中的标准千兆模块分为两种：千兆 GBIC 扩展模块和千兆 SFP 扩展模块。

千兆接口转换器模块(Gigabit Interface Converter ，简称：GBIC)，适用于光纤接头为 SC 的线路应用。支持的模块型号及接口标准如下所示。

模块型号	接口标准	适用产品型号
TOPSEC-GBIC-SX	1000Base-SX	千兆系列防火墙、VPN、UTM、IDS/IPS、审计系统等产品， (如 TG-5407, TG-5307, TG-5207, TG-507-UTM,TV-6807, TS-3205-IDS, TA-507-Watch)
TOPSEC-GBIC-LX	1000Base-LX	
TOPSEC-GBIC-ZX	1000Base-ZX	
TOPSEC-GBIC-T	1000Base-T	

小封装可插拔模块（Small Form-Factor Pluggable, 简称：SFP），一种小型的接口转换器，适用于光纤接头为 LC 的线路应用。支持的模块型号及接口标准如下所示。

模块型号	接口标准	适用产品型号
TOPSEC-SFP-SX	1000Base-SX	千兆系列防火墙、VPN、密码机、UTM、审计系统等产品 (如 TG-5466, TG-5366, TG-5266, TG-5328, TG-4628, TG-566-UTM, TV-6866, SJW11-A-F)
TOPSEC-SFP-LX	1000Base-LX	
TOPSEC-SFP-ZX	1000Base-ZX	
TOPSEC-SFP-T	1000Base-T	

3．专用千兆模块

网络卫士防火墙适用的专用千兆模块为天融信公司产品专用，必须配合天融信的千兆产品使用。

专用 GBIC 的模块型号及接口标准如下所示。

模块型号	接口标准	适用产品型号
TOPSEC-GBIC-AUTO	10/100/1000BASE-T	千兆防火墙、VPN、UTM、审计系统等产品 (如 UTMTG-5407, TG-5307, TV-6807, TG-507-UTM, TA-507-Watch)

提示

- ✧ 在网络卫士系列防火墙中，并非所有产品型号均支持扩展模块，某些低端防火墙上没有扩展插槽。
- ✧ 不同扩展模块的接口模块规范和安装/拆卸过程等详细介绍请参见《Topsec 扩展模块安装指南》。

声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。
3. 本安装手册中的安装方法、步骤为天融信建议使用，并非唯一和必须的安装途径，请客户参考使用。
4. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
5. 本手册中提到的信息为正常公开的信息，若因本安装手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。